Cyber Security Handbook for Small Business and Not-for-Profit Directors

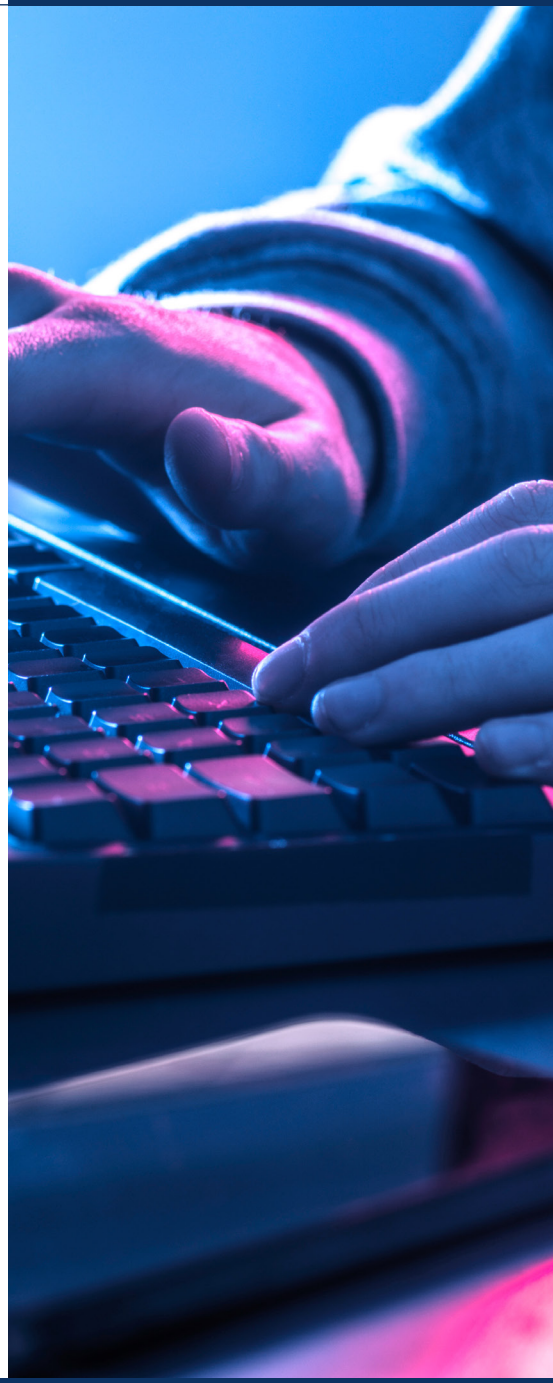
Australian Information Security Association
Australian Institute of Company Directors

A JOINT PUBLICATION BY

Australian Institute of Company Directors

AISA Australian Information Security Association

Contents



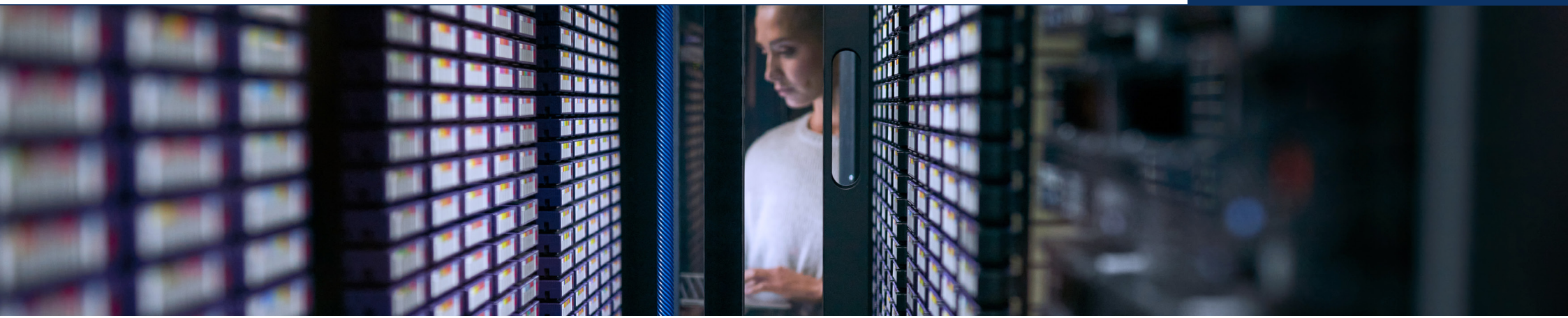
Introduction

Over recent years the profound consequences of serious cyber incidents have impacted every part of the Australian community. Systems have been compromised, personal data has been stolen, commercially sensitive information has been compromised, and cyber security has become a significant concern for all Australians. This dynamic is not just relevant to large Australian companies but also small and medium size enterprises (**SMEs**) and not-for-profits (**NFPs**).

Directors of all sizes of organisations have a key governance role to play in being aware of the cyber threat landscape, prioritising cyber resilience at their organisations, and developing capabilities for the oversight of cyber risk and effective responses to cyber crises.

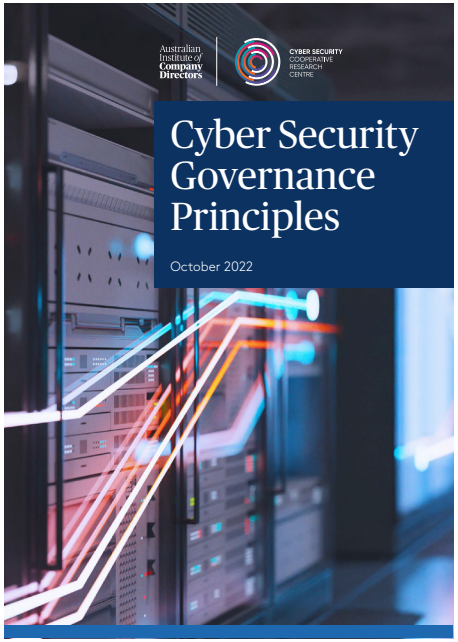
The vast majority of businesses in Australia are SMEs, including small NFPs and charities, and their cyber security capabilities are different to those of larger enterprises. SMEs and small NFPs often have limitations on their capabilities and resources which can impact how much effort they can put into managing their cyber security. Therefore, any approach that an SME takes to cyber security needs to be aligned with business objectives. With that said, there are a great number of cyber security controls and processes that require low cost and resources which can be employed to help build the resiliency of SMEs.

The Australian Information Security Association (**AISA**) and the Australian Institute of Company Directors (**AICD**) have collaborated to assist the directors of SMEs and NFPs to enhance the cyber security posture of these businesses without introducing unnecessary complexity or operational burden. The guidance is drafted to have application to a broad population of SMEs and NFPs and is not solely intended for organisations involved in digital or technology focused industries.



As small organisations routinely contend with juggling priorities amidst constrained human and financial resources, this guide aims to assist directors build foundational cyber resilience. Through providing clear and concise recommendations for easy implementation, this guide is intended to complement the detailed Australian Signals Directorate's (**ASD**) **Essential Eight** maturity model, other key cyber security guidance, and the **AICD CSCRC Cyber Security Governance Principles**.

While not exhaustive, this guide can be used to substantially strengthen an organisation's cyber security capabilities, offering crucial insights to mitigate the risk of SMEs and NFPs falling victim to cyber threats.



THE ROLE OF THE SME DIRECTOR IN AN ELEVATED CYBER THREAT ENVIRONMENT

As a director of an SME or NFP, it can be overwhelming trying to keep up with the ever-shifting cyber threat environment. Many directors may be unsure of the role they need to play in contributing to the organisation's cyber strategy, implementing frameworks such as the Essential Eight, or responding effectively to incidents.

As a director, the role you take with regards to cyber security in your organisation is the same you would take to oversee any other risk impacting your business. Your duties and obligations do not change if you are an owner director, executive director or serve as a director in a volunteer capacity (e.g. on the board of a NFP). This means that as a director, ensuring appropriate cyber risk treatments are in place, investments are made in the areas that require it, and company policies are set and understood.

The summary of the core directors' duties in the *Corporations Act 2001* as they relate to cyber security is detailed in the accompanying box, taken from the **AICD CSCRC Cyber Security Governance Principles.**

As directors, you may not have specialised knowledge about cyber security. However, that does not reduce the standard of care you need to apply. The same applies if you are not an expert in finance or law. Directors may rely on the advice of others or can delegate; however, you need to ensure you are still obtaining and understanding all the information you need to make a well-informed decision.

Governing for cyber risks and building an organisation's cyber resilience forms part of directors' existing fiduciary duties owed to the company under both common law and the Corporations Act 2001 (Cth) (**Corporations Act**).

Duty to act with care and diligence	Directors have a duty to act with care and diligence to guard against key business risks. This includes ensuring appropriate systems are in place to bolster cyber resilience, as well as prevent and respond to cyber incidents.
Duty to act in good faith and in the best interests of the corporation	Directors must exercise their powers and discharge their duties in good faith in the best interests of the company, and for a proper purpose. In making decisions on cyber security on behalf of the company, directors must consider the impact of those decisions on shareholders/members and stakeholders including employees, customers, suppliers, and the broader community.
Reliance on information and advice provided by others	Just because a director does not have specialist knowledge about cyber security does not mean that the director's standard of care is reduced. While in some circumstances, directors may rely on information or the advice of others, or delegate certain cyber matters to a board committee or management roles, this does not absolve directors of their accountability for decision-making.
Other statutory obligations	Directors of entities that hold an Australian Financial Services License (**AFSL**) are also subject to general and specific obligations under the Corporations Act. A recent decision of the Federal Court of Australia, ASIC v RI Advice, confirmed this includes having in place risk management systems and controls to manage business risks. APRA regulated entities are also subject to extensive prudential obligations relevant to cyber security risk.
Duty to advise the market where there is an effect on a company's share price	For companies listed on the Australian Securities Exchange (**ASX**), directors must advise the market immediately if the company becomes aware of any information would have a material effect (positive or negative) on the company's share price. In the cyber context, this might apply in the event of customer data loss as a result of a significant cyber incident. This type of event may also expose a company and/or its directors to the risk of a class action.

In addition to being aware that director duties are relevant to the oversight of cyber security risks, an SME director should ensure they are aware of the legal obligations that are relevant to the management and protection of information and information systems:

- The Department of Home Affairs has published a comprehensive reference document, **Overview of Cyber Security Obligations for Corporate Leaders**, for directors and senior management on key regulatory obligations that are relevant to cyber security settings. The key obligations are categorised by preparedness, reporting and response. Key regulatory regimes include the *Privacy Act 1988* (**Privacy Act**) and *Security of Critical Infrastructure Act 2018*.
- For most directors, the Privacy Act 1988 (**Privacy Act**) is the key regulatory regime that is relevant to how their business collects and protects personal information. Although, it is important to note that there is a small business exemption for the application of the Privacy Act that means that most businesses with a turnover less than $3 million per annum are not covered by its obligations. More information on the exemption, including which businesses are not exempt, is available in the **Privacy Act**. The accompanying box provides a summary of the key elements of the Privacy Act.
- Further information on director duties and legal obligations can be found in the AICD CSCRC **Cyber Security Governance Principles**.

In addition, there are industry-specific regulations that board directors should be aware of as part of their fiduciary duties. These regulations depend on the industry. For example, healthcare organisations should comply with the *My Health Records Act*, and financial institutions adhere to the Australian Prudential Regulation Authority prudential requirements.

A director should stay informed about regulatory developments and emerging cyber threats which are overarching and specific to their organisation's industry.

Taking time to learn, review information and knowing what questions to ask are skills that will serve you well in your role as a director. A crucial element in the governance of cyber security risk is for directors to adopt a hands-on approach by requesting "show me how" instead of settling for explanations with "tell me how." A simple report that can show the ongoing management of security controls can be very effective.

THERE ARE TWO KEY REGIMES UNDER THE PRIVACY ACT THAT DIRECTORS SHOULD BE AWARE OF IN THEIR OVERSIGHT OF CYBER SECURITY:

1. Notifiable Data Breaches (NDB) scheme – requiring an organisation to notify affected individuals and the Office of the Australian Information Commissioner (OAIC) as soon as practicable of a material data breach.
2. Australian Privacy Principle 11 – Security of Personal Information (APP 11) – requiring an organisation to take active measures to ensure the security of personal information it holds.

Cyber Security 101: Fundamentals for SMEs & NFPs

Fundamentals encompass the essential and indispensable aspects of a baseline cyber security posture. The recommendations in this section offer building blocks that a director should oversee in building a cyber-secure environment for their organisations.

1. Compile an inventory of all Information Technology assets and services in your business, including hardware (laptops, computers, etc.), software systems (business applications), and any cloud service providers. Maintaining an asset list facilitates efficient tracking and awareness of the technology endpoints present in your business.
2. Undertake a data stocktake that provides visibility of the key data that is collected from customers, suppliers and employees, where the data is stored, who has access to the data, and how it is deleted. Establish an understanding of the significance of the data for the business and the potential repercussions of a breach of this information.
3. Implement access and authorisation controls, including through creating unique logins for each staff member using computer systems and restrict administrative privileges to essential personnel only. Using the principle of least privilege, staff access should be limited to the minimum required to do their duties.
4. Protect all logins to computer systems with passkeys or unique and complex passwords with multi-factor authentication (**MFA**) where possible. When using MFA, choose a methodology that is resistant to phishing. For example, opt for the use of Authenticator apps as opposed to relying on text messages or emails for code verification.

5. Make sure that all software and firmware is kept up-to-date through installing automatic updates from trusted software, hardware, and service providers. Assess risk and ensure computer systems (laptops and computers) have anti-virus software installed.
6. Maintain physical backups of key systems, software and data that is isolated to ensure access as required in the event of an incident.
7. Conduct practical employee training that will allow staff to understand risks and how to identify potential malicious email and social engineering attempts.
8. A mobile device policy is key to ensure that all staff or volunteers understand what is expected of them regarding the use of mobile devices and how they access company systems.
9. A **cyber incident response plan** is an essential document for all businesses to ensure that in the event of an incident, responders know what is required and who needs to be notified of an event. Workshops, mock exercises, and regular reviews of this plan are needed to ensure they are as up to date as possible and practical in handing an incident.
10. As suggested in ASD's ACSC guide on **securing customer personal data for small to medium businesses**, event logging can be an important component of an organisation's cyber protection, and should be considered. It can be used to detect access breaches, and storing the log data in a secure fashion is important to assist with post-cyber incident forensics and analysis.
11. Contemporary IT systems and software typically come equipped with out-of-the-box support for passwords, passkeys, and MFA. In cases where an application or system lacks these features, it is advisable to notify the vendor or provider, urging them to incorporate these functionalities as standard requirements. In addition, SME directors should encourage management to shop around and see what options are available that best suits the cyber security requirements of the organisation.
12. Establish and maintain contact with security related professional associations, forums, and interest groups. Some examples include ASD's Cyber Security Program, and AISA Corporate Partnership and membership. Choose one that suits your organisation.

Further guidance for SMEs can be found in the ASD's **ACSC Small Business Cyber Security Guide**, **Australian Charities and Not-for-profits Commission (ACNC) Governance Toolkit: Cyber Security**, and separately the **AICD CSCRC SME and NFP Director Checklist**.

PASSWORD AND PASSPHRASE BEST PRACTICE

Many small businesses face cyber attacks as a result of poor password behaviours. For example, reusing the same password on multiple accounts.

SMEs & NFPs should use password managers and passphrases to create strong passwords.

A password manager acts like a virtual safe for your passwords. You can use it to create and store strong, unique passwords for each of your accounts.

For accounts that you sign into regularly, or that you otherwise do not want to store in a password manager, consider using a passphrase as your password.

Passphrases are a combination of random words, for example 'crystal onion clay pretzel'. They are useful when you want a secure password that is easy to remember. Use a random mix of four or more words and keep it unique – do not reuse a passphrase across multiple accounts.

This guidance is taken from the ASD's **ACSC Small Business Cyber Security Guide**.

Building a culture of cyber resilience

Directors have a key role in setting a tone from the top in promoting a cyber resilient culture across the organisation. Consistent and regular communications, testing, and education is essential to equip staff with the knowledge needed to navigate safely in the digital world.

Cyber awareness should not be treated as an annual checkbox for compliance but rather as an ongoing commitment. The **AICD CSCRC Cyber Security Governance Principles** has extensive guidance on promoting a culture of cyber resilience. Some of the best practices that SMEs and NFPs can consider are:

1. Mandatory training and phishing testing for all employees and volunteers where appropriate.
2. Pick a staff member to be a 'cyber security leader' to promote strong cyber practices and respond to questions from other staff.
3. Subscribe to ASD's cyber security alert service to stay across emerging cyber threats (**Sign up for alerts | Cyber.gov.au**).
4. Monitor the Industry Live News feed on **AISA's website** to stay informed about the latest industry news and alerts.

Simple measures include subscribing to online platforms that provide regular training videos or activities. Select content that is not only educational but also engaging, ensuring that employees not only fulfill training requirements but also retain and apply the information. The training should focus on altering staff behaviour and their response to security incidents.

While people are often labelled as the weakest link in cyber security, with the right support, employees and volunteers (in the case of NFPs and charities) can become a robust line of defence against threats. By investing in ongoing education and improvement, employees can play a crucial role in reducing response times and potentially preventing incidents altogether.

Providing guidance on recognising phishing attempts, promoting safe browsing practices, and emphasising the importance of reporting suspicious activities are vital topics to cover. Empowering staff with this knowledge enables them to be proactive in responding to cyber threats and enhances the overall cybersecurity posture of the organisation.

Council of Small Business Organisations Australia (**COSBOA**) has undertaken a national initiative to change the behaviours of Australia's 2.3 million small businesses and created a new Cyber Wardens program resource toolkit and training. Cyber Wardens is the online version of first aid officers or fire safety wardens, who can prevent, prepare, fight, and help recover from a cyber-attack or the theft of customer data or intellectual property. More information is available at **COSBOA's Cyber Wardens page**.

Risk management

Cyber risk, despite its prominence and velocity, is still an operational risk that should fit within an SME's existing approach to risk management.

While cyber risk cannot be reduced to zero there are several accessible and low-cost controls that all SME's can utilise to build cyber resilience. SME directors should regularly assess the effectiveness of cyber controls to account for a changing threat environment, technological developments, and the organisation's capabilities.

POLICIES AND PROCESSES

Documenting key internal policies and processes is an integral part of managing cyber security across an organisation. The development of policies and processes should not take up excessive time and resources, nor do they need to be overly long, bureaucratic, or complex. Rather, the policies should involve establishing practices to ensure that information technology and digital assets and data are secure, as well as ensuring staff awareness of acceptable usage and safe practices when using technology and systems.

These processes include setting key roles and responsibilities for cyber security in the SME or NFP and ensuring appropriate reporting mechanisms are in place so that you can make well-informed decisions on risk, strategy, and incident response. In a small business, roles and responsibilities will need to be tailored to how the organisation operates. For example, if you have a team of five people, some people may have several roles and multiple responsibilities. In this setting, you as the director may have the combined responsibilities of leading the incident response team, communicating with clients and third party support, as well as managing the staff's well being.

The **AICD CSCRC SME and NFP Director Checklist** (a component of the Cyber Security Governance Principles) contains a list of practical, low cost cyber risk controls.

Establishing a foundational information security policy is essential to articulating the SME's position on third party cyber risk management.

THIRD-PARTY CYBER RISK MANAGEMENT

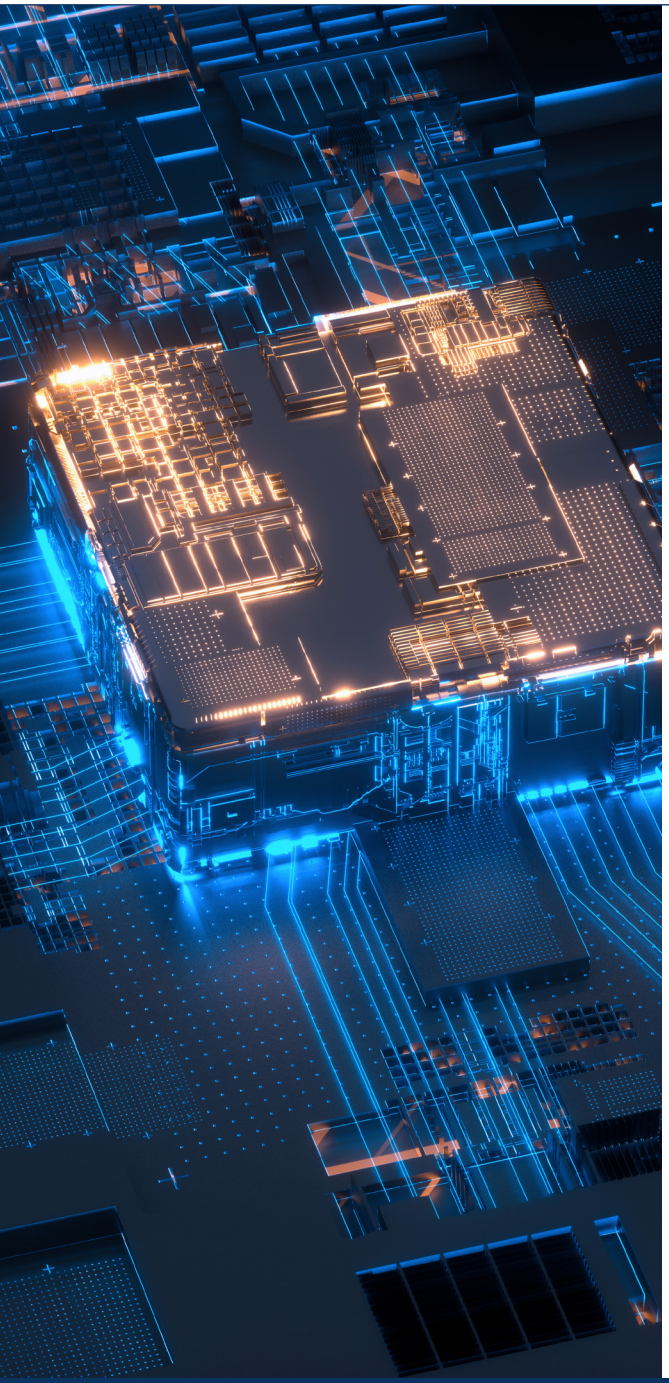
Third-party cyber risk management refers to the processes, strategies, and controls an organisation puts in place to oversee and interact with external entities, such as vendors or service providers, with the goal of ensuring that these third parties operate in alignment with the organisation's expectation of how cyber security will be managed.

In many instances it may not be possible for an SME or NFP to negotiate terms or elements of service agreements with key systems, software, and IT infrastructure providers. The size of these third parties, for instance Software as a Service (SaaS) providers, means that a small business will have to 'take' the offered terms and conditions.

However, where possible the directors of an SME should have oversight of whether the key agreements have the following elements:

- Limit the use of, and access to the systems and information based on the purpose of the engagement.
- A right to conducting basic risk assessments and due diligence on the service provider, particularly if they are handing information or have access to systems.
- Establish processes to monitor performance on data protection and cyber security controls.
- Business continuity and disaster recovery planning and coverage.
- Confidentiality or non-disclosure agreements.
- Data retention, recovery, and backups.
- Roles and responsibilities – especially with regards to incident response.
- Appropriate indemnities, warranties, and disclaimers.

While control over the agreement and terms of use may be limited, appropriate due diligence assists directors to fully understand the risks and opportunities from a security perspective. This in turn allows more informed decisions in line with the organisation's risk appetite and business objectives. Effective third-party cyber risk management is crucial for SMEs and NFPs to mitigate risks, protect sensitive information, and maintain overall operational resilience.



KEEP EVERYTHING UPDATED

An SME director should be confirming that the organisation is vigilant in updating computer systems, software, hardware, services, and applications to the latest versions. This ensures the SME has the latest security patches, reducing the risk of cyber vulnerabilities.

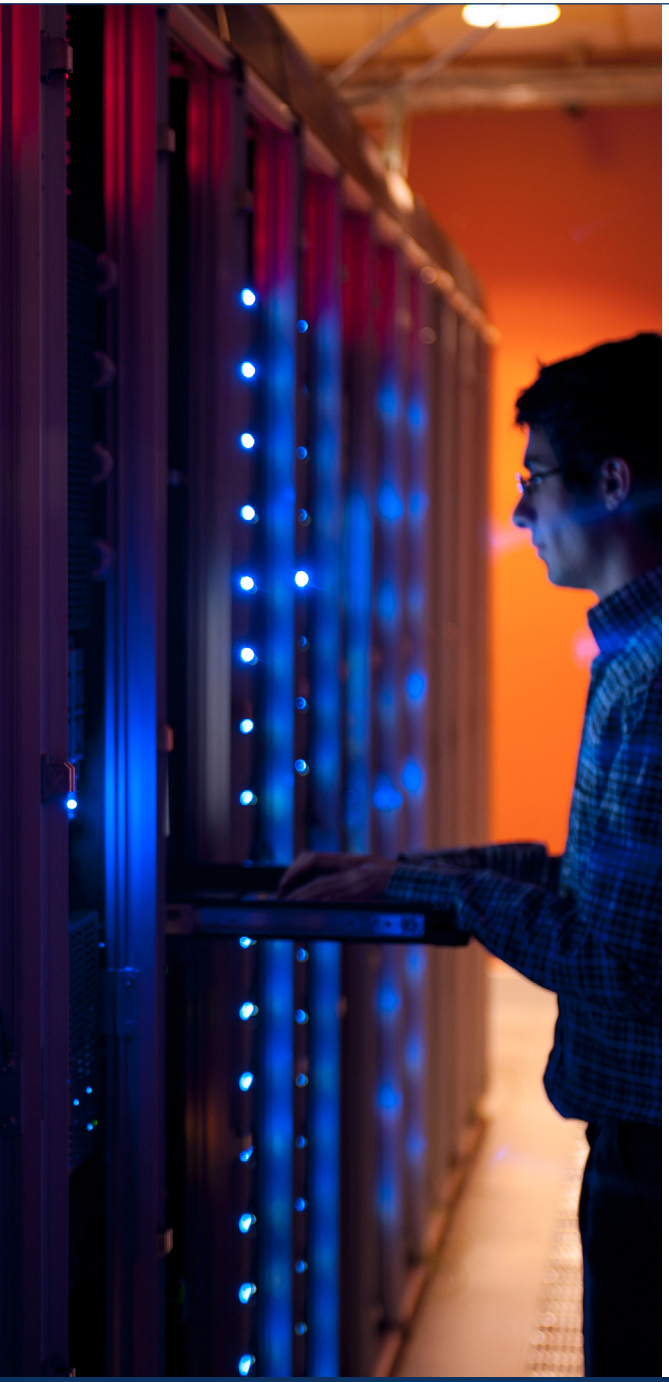
A large percentage of breaches are due to vulnerabilities that have not been patched, or vulnerabilities that have patches available, but have not been applied.

In most SMEs, where systems can often be patched with minimal disruption, prompt updates significantly enhances cyber security posture, shielding the business from known vulnerabilities.

Key actions to ensure effective updates include:

- Nominating an individual staff member with direct responsibility for ensuring all key software and digital assets are up-to-date.
- Regularly updating systems and platforms and turning on automatic updates.
- Establishing and adhering to a consistent update schedule.

In addition, maintaining documented records of the systems in use (Information technology assets and services register) facilitates quick assessments of the current patching status, ensuring a proactive approach to cyber security. Most vendors and providers have these updates and patches available from their website and provide basic guidelines that should be followed to install these updates.



SECURE WHAT IS IMPORTANT TO YOU

A key role for the directors with respect to cyber security is having clear visibility of what digital assets and data are key to the business and understanding how these are protected. This role includes understanding what data is flowing across which systems, and how it is being secured both at rest (in storage) and in transit.

This information plays a crucial role in business, serving as a primary means of interaction with staff, clients, and vendors. The content of this information is often highly sensitive, and the potential loss of such information could pose significant challenges for a small organisation. Some scenarios to consider are:

- Information that is considered commercially sensitive.
- Data that includes personally identifiable information, which if breached can cause serious harm to individuals, and in some circumstances will trigger mandatory notification obligations under the Notifiable Data Breaches Scheme and reporting to other stakeholders and regulators.
- Cyber security incidents where an attacker gains unauthorised access to business information and uses it for deceiving, manipulating data, or defrauding the business or its stakeholders.
- Ensuring secure encrypted storage and transfer of information, especially when sharing sensitive documents.
- Staff awareness against compromise tactics such as impersonation, fraudulent requests, invoice frauds, and phishing.
- Access controls to restrict who can view, edit, or share specific information.
- Monitoring activities for any unusual or suspicious behaviour. Ensure that access logs and permissions are regularly audited to ensure they align with business requirements. If your business does not have these skills internally, leverage the expertise of your IT service provider to assist with these tasks.

BACKUP YOUR DATA

A SME director should ensure the business is regularly backing up crucial business information and systems. Best practice is for these back-ups to be in a separate location which can be accessed when the original form of the information is impacted. This may mean having backups in off-site protected storage, or in a separate cloud environment to the one used for the primary storage of the information. Backups should be regularly reviewed and tested to ensure the information and systems can be successfully restored if necessary. In the event of a ransomware attack or device failure, the ability to restore systems to their last operational state becomes essential.

Steps to ensure comprehensive backup of important business data include:

- Identify critical data necessary for business operations across all systems.
- Determine backup process and the supporting technology.
- Determine the frequency of backup schedules based on the acceptable data loss threshold.
- Ensure regular backups of all platforms integral to business operations, including cloud services like Google Workspaces or Microsoft 365. Note that cloud providers typically do not automatically backup systems unless specified and paid for as a service.
- Test backups regularly to instil confidence in the business's ability to restore from them.
- Keep backup copies separate from main systems to guard against the scenarios leading to system unavailability.

Consider backups as an insurance policy; they serve as a reliable resource to swiftly restore operations and minimise disruptions when unforeseen issues arise.

ASD has extensive cyber security guidance on **how to back up your files and devices**.

INSURANCE

Insurance is an area that directors need to pay particular attention to. Each policy is different, and knowing what to look for is incredibly important. Additionally, each SME's needs will vary. Not all policies cover the spectrum of cyber security incidents you may encounter, so knowing ahead of time exactly what you are covered for is important for your incident response planning.

Depending on your policy, your insurance provider may require you to engage incident response assistance from their selected providers. This could mean engaging their recommended forensic experts, lawyers, or security consultants. In addition to this, they may have specialists who can assist with cyber security incidents that involve ransomware. This means that, as a director, you have more options to work with to help you through such an incident.

Cyber Security Incident Response Planning

Directors of organisations of all sizes, including SMEs and NFPs, must be prepared for the genuine possibility that their organisation will experience a cyber security incident. Cyber security incidents vary in impact and likelihood. How well an organisation can respond to a cyber security incident depends on their preparedness. SMEs run the risk of facing various types of cyber security incidents with varying levels of criticality. Key incidents that SMEs should concern themselves with include data loss, ransomware, extortion, critical technology and system failures, access to information by unauthorised parties, denial of service to systems or websites, and exploiting critical vulnerabilities. Because of all the ways an SME's information or systems can be compromised, the question should not be whether an incident will occur, but rather, when?

This paradigm underscores the inevitability of cyber incidents, emphasising the importance of proactive preparation and knowing how to respond effectively when they occur. A Cyber Incident Response Plan (**Response Plan**) is a document that details the steps an organisation can follow when responding to and managing a cyber security incident or any other disruptive event. The primary objective of a Response Plan is to minimise damage, communicate effectively, and reduce recovery time and costs.

The AICD publication **Governing Through a Cyber Crisis: Cyber Incident Response and Recovery for Australian Directors** provides practical guidance for directors of all sizes of organisations on how to prepare for and govern during a significant cyber security incident, such as a ransomware attack or the failure of key operating systems.

SME directors should work with management to ensure the Response Plan is as comprehensive as necessary to prepare against adverse or disruptive events. In a cyber incident an SME director may play a more active role, including communicating with clients, third party support as well as overseeing employee and volunteer well-being.

The Response Plan should be saved as a hard copy for reference, and should typically include:

- Roles and responsibilities for managing the incident.
- What internal resources may need to be called upon.
- Who can be called upon externally for assistance.
- Communication plan(s) for customers, media, regulatory bodies such as ASD's ReportCyber, and internally.
- Which systems will need to be restored and the time frame in which this needs to occur.
- Post incident reviews and corrective action plans to prevent similar cyber security incidents in the future and to rebuild reputation.

Regular testing, training, and updates are essential to maintaining the plan's effectiveness. The goal is to respond swiftly, efficiently, and effectively to any incident, thereby minimising the impact.

Summary

This guide is intended to provide directors of SMEs and small NFPs with an understanding of the key components of building cyber resilience to protect the organisation, clients, employees, and other key stakeholders from the ever-increasing cyber security threats.

This guide has been developed by cyber security leaders and company directors who have a keen knowledge of how to build cyber security programs for businesses of all sizes.

Many organisations go out of business each year due to a cyber incident or data breach. Take this guide as a reminder that even though it is your responsibility to ensure your organisation remains resilient, you are not alone in the fight against the cyber threats we all face.

Resources and further assistance

- Glossary of key terms (ASD)
- AISA Ask a Cyber Security Expert
- Essential Cyber Security – Essential Eight
- AICD CSCRC Cyber Security Governance Principles
- AICD CSCRC Ashurst Governing Through a Cyber Crisis
- ASD's ACSC Cyber Resources for Small Businesses
- ASD's ACSC Small Business Security Guide
- ASD's Cyber Security Partnership Program
- ASD's ACSC Protecting Your Business and Employees
- Australian Information Security Association (AISA) Membership
- ASD's ACSC How to Backup your Files and Devices
- ASD's ACSC Cyber Alert Service
- AISA Boards and Cyber Resilience Survey Findings
- COSBOA's Cyber Security Management Solutions for SME's
- COSBOA Cyber Wardens
- eSafety Industry Assessment Tools
- ASD's ACSC Securing Personal Data for Small to Medium Businesses
- ACNC Governance Toolkit: Cyber Security
- CISC Overview of Cyber Security Obligations for Corporate Leaders

Appendix: Example one page cyber policy statement

POLICY STATEMENT

This IT Systems Usage Policy outlines the acceptable use of information technology resources.

SCOPE

This policy applies to all individuals granted access to IT systems, including employees, contractors, and any other authorised users.

AUTHORISED USE

IT systems and resources are to be used solely for business-related activities. Personal use should be restricted.

Users must comply with all applicable laws and regulations, including but not limited to copyright laws, software licensing agreements, and data protection regulations.

SECURITY AND ACCESS

Users are responsible for the security of their login credentials. Sharing of login credentials is strictly prohibited.

Access to sensitive information should be on a need-to-know basis. Users are only authorised to access data and systems required for their job responsibilities.

Attempting to access unauthorised areas of the IT systems or using another user's account without permission is strictly prohibited.

DATA PROTECTION

Users must respect the privacy of sensitive and confidential information. Unauthorised disclosure or sharing of such information is prohibited.

All critical business data must be regularly backed up. Users are responsible for ensuring their data is stored in approved locations.

SOFTWARE AND HARDWARE

Only authorised IT personnel may install software on company systems. Employees must not install unauthorised software.

Company-owned hardware is to be used for business purposes only. Personal devices should not be connected to company networks without approval.

INTERNET AND EMAIL

Internet access is provided for business purposes. Employees should refrain from accessing inappropriate or non-business-related websites.

Use company email responsibly. Avoid sending confidential information via unsecured channels and be cautious of phishing attempts.

CONSEQUENCES OF VIOLATION

Violations of this policy may result in disciplinary action, including but not limited to warnings, suspension, or termination. Legal action may be taken in cases of severe violations.

ABOUT AICD
The Australian Institute of Company Directors is committed to strengthening society through world-class governance. We aim to be the independent and trusted voice of governance, building the capability of a community of leaders for the benefit of society. Our membership includes directors and senior leaders from business, government and the not-for-profit sectors.

ABOUT AISA
The Australian Information Security Association (AISA) is the nationally recognised peak body for cyber security with a membership of over 12,000 individuals and corporate partners nationwide. AISA is a registered charity with deductible gift recipient (DGR) status for its scholarship fund. Our vision is to promote an environment where all individuals, businesses, and governments are well-informed of the risks of cyber security and are prepared to take all necessary measures to protect against such threats.

DISCLAIMER
The material in this publication does not constitute legal, accounting or other professional advice. While reasonable care has been taken in its preparation, the AICD does not make any express or implied representations or warranties as to the completeness, reliability or accuracy of the material in this publication. This publication should not be used or relied upon as a substitute for professional advice or as a basis for formulating business decisions. To the extent permitted by law, the AICD excludes all liability for any loss or damage arising out of the use of the material in the publication. Any links to third party websites are provided for convenience only and do not represent endorsement, sponsorship or approval of those third parties, any products and services offered by third parties, or as to the accuracy or currency of the information included in third party websites. The opinions of those quoted do not necessarily represent the view of the AICD. All details were accurate at the time of printing. The AICD reserves the right to make changes without notice where necessary.

COPYRIGHT

For more information about AISA AICD Cyber Security Handbook, please contact:

T: 1300 739 119
E: **nsw@aicd.com.au**

JOIN OUR SOCIAL COMMUNITY

aicd.com.au

CCT709